



Los mejores 10 consejos para protegerse del robo de identidad

INFORMACIÓN PARA EL CONSUMIDOR, HOJA 1

Un ladrón de identidad toma su información personal y la usa sin que usted se entere. El ladrón puede incurrir deudas e incluso cometer delitos a nombre suyo. Los siguientes consejos pueden ayudarlo a reducir el riesgo de convertirse en víctima.

1. Proteja su número de Seguro Social

No cargue su tarjeta del Seguro Social en su billetera. Si su plan médico (que no sea Medicare) o otra tarjeta se basa en el número del Seguro Social, pídale a la compañía un número diferente. Si desea más información, vea: “Su número de Seguro Social: Cómo controlar la llave del robo de identidad” (*Your Social Security Number: Controlling the Key to Identity Theft*) (Información para el consumidor, hoja 4) en nuestra página Web sobre Números de Seguro Social.

2. Combata el “phishing”: no muerda el anzuelo.

Los timadores buscan víctimas haciéndose pasar por bancos, tiendas o dependencias de gobierno. Esto lo hacen por teléfono, por correo electrónico o por correo regular. Nunca dé su información personal, a menos que usted mismo haya iniciado el contacto. No responda a ninguna solicitud para verificar su número de cuenta o contraseña. Las compañías legítimas nunca solicitan ese tipo de información en este modo.

3. Impida que su identidad se vaya a la basura.

Triture o rompa concienzudamente los papeles que contienen datos personales antes de echarlos a la basura. Triture los ofrecimientos de tarjetas de crédito y de “cheques de conveniencia” que no utilice.

4. Controle su información financiera personal.

Las leyes de California requieren que bancos y otras compañías de servicios financieros le pidan autorización para compartir sus datos financieros personales con compañías externas. Usted también tiene el derecho de limitar la información personal que se comparta con las afiliadas de su compañía. Si desea más información, consulte “Su privacidad financiera” (*Your Financial Privacy*) (Información para el consumidor, hoja 2) en nuestra página Web sobre Privacidad Financiera.



5. Proteja su computadora contra los virus y espías.

Proteja su información personal en su computadora casera. Use contraseñas sólidas: por lo menos de ocho caracteres, combinando letras, números y símbolos, que sea fácil de recordar para usted, pero difícil de adivinar para los demás. Use software de protección, como firewall, antivirus y anti-spyware, y actualícelo con regularidad. Manténgase alejado del spyware. Descargue software sólo de sitios que usted conozca y en los que confíe. Nunca instale software sin saber para qué es. Ponga el nivel de seguridad de su navegador, por ejemplo Internet Explorer, por lo menos en “media”. No haga clic en vínculos de ventanas emergentes ni de mensajes de correo electrónico spam.

6. Cuidado al hacer clic.

Al comprar en línea, revise el sitio Web antes de introducir el número de su tarjeta de crédito y otros datos personales. Lea la norma de privacidad y busque si hay oportunidad de evitar que compartan su información. (Si no hay norma de privacidad, ¡cuidado! Mejor compre en otra parte.) Introduzca sus datos sólo en páginas Web seguras, con el nombre “https” en la barra de dirección y el símbolo del candado cerrado en la parte de abajo de la ventana del navegador. Esas son las señales de que sus datos serán encriptados o codificados, lo que los protege de los piratas.

7. Revise sus cuentas y estados de cuenta del banco.

Abra de inmediato las cuentas de la tarjeta de crédito y los estados de cuenta bancarios. Revise con cuidado para ver si hay cargos o retiros no autorizados y repórtelos de inmediato. Llame si no le llegan las cuentas a tiempo. Eso podría significar que alguien le cambió la información de contacto para ocultar cargos fraudulentos.

8. Detenga los ofrecimientos de crédito preaprobado.

Detenga la mayoría de los ofrecimientos de tarjetas de crédito preaprobadas. Constituyen un tentador blanco para los ladrones de identidad que roban el correo. Haga que retiren su nombre de las listas de mercadotecnia de las agencias de información sobre antecedentes de crédito. Llame sin costo al 888-5OPTOUT (888-567-8688).

9. Haga preguntas.

Haga preguntas siempre que alguien le pida información personal que parezca inapropiada para la transacción. Pregunte cómo se utilizará la información y si será compartida. Pregunte cómo será protegida. Explique que usted está preocupado por el robo de identidad. Si usted no está satisfecho con las respuestas, considere la posibilidad de ir a otro lugar.

10. Revise su reporte de crédito: es gratis.

Una de las mejores formas de protegerse del robo de identidad es vigilar su historia de crédito. Usted puede recibir un reporte de crédito gratuito cada año de cada una de las tres agencias nacionales de información sobre antecedentes de crédito: Equifax, Experian y TransUnion. Solicite los tres reportes al mismo tiempo, o conviértase en su propio servicio de monitoreo de crédito sin costo. Simplemente reparta sus solicitudes, ordenándolas de una agencia diferente cada cuatro



meses. (Las agencias de crédito ofrecen servicios de monitoreo más exhaustivos que cuestan de \$44 a más de \$100 al año.) Ordene su reporte de crédito anual por teléfono, larga distancia sin costo, al 1-877-322-8228 o en línea en www.annualcreditreport.com. También puede enviar por correo su formulario de pedido. Vea nuestra Información para el consumidor, hoja 10, “Cómo congelar sus archivos de crédito” (*How to Freeze Your Credit Files*).

Esta hoja informativa es para efectos ilustrativos y no debe interpretarse como consejo legal ni como normas del estado de California. Si usted desea asesoramiento o un consejo sobre un caso en particular debe consultar a un abogado u otro especialista. Esta hoja puede copiarse si (1) no se cambia ni tergiversa el significado del texto copiado, (2) se da crédito a la Oficina de Protección de la Privacidad de California y (3) todas las copias se distribuyen sin costo.